

Roc'd PCT/PTO 20 DEC 2004

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



10/518639

(43) Date de la publication internationale
31 décembre 2003 (31.12.2003)

PCT

(10) Numéro de publication internationale
WO 2004/002058 A2

(51) Classification internationale des brevets⁷ : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR2003/001871

(22) Date de dépôt international : 18 juin 2003 (18.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/07688 19 juin 2002 (19.06.2002) FR

(71) Déposant (pour tous les États désignés sauf US) : GEM-
PLUS [FR/FR]; Parc d'Activités de Gémenos, Avenue du
Pic-de-Bertagne, F-13420 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : FEYT,
Nathalie [FR/FR]; 8, chemin de Raphèle, 7 lotissement
l'Oliveraie, F-13780 Cuges les Pins (FR). JOYE, Marc
[FR/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).

(74) Mandataire : AIVAZIAN, Denis; Gemplus la Vigie, Ser-
vice brevets, BP 100, F-13705 La Ciotat Cedex (FR).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE,
SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,
TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à l'identité de l'inventeur (règle 4.17.i)) pour les
désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA,
BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE,
DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR,
HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,
LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI,
NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL,
TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM,
ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ,
TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ,
MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY,
CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,
NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— relative au droit du déposant de demander et d'obtenir un
brevet (règle 4.17.ii)) pour les désignations suivantes AE,
AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA,
CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL,
PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT,
TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO
(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES,
FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI,
SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GQ, GW, ML, MR, NE, SN, TD, TG)

[Suite sur la page suivante]

(54) Title: METHOD OF GENERATING ELECTRONIC KEYS FOR A PUBLIC-KEY CRYPTOGRAPHY METHOD AND A
SECURE PORTABLE OBJECT USING SAID METHOD

(54) Titre : PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE
PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN OEUVRE LE PROCEDE

(57) Abstract: The invention relates to a method of generating electronic keys (d) for a public-key cryptography method using an
electronic device. The inventive method comprises two separate calculation steps, namely: step A consisting in (i) calculating pairs
of prime numbers (p, q), said calculation being independent of knowledge of the pair (e, l) in which e is the public exponent and l is
the length of the key of the cryptography method, and (ii) storing the pairs thus obtained; and step B which is very quick and can be
executed in real time by the device, consisting in calculating a key d from the results of step A and knowledge of the pair (e, l).

(57) Abrégé : L'invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au
moyen d'un dispositif électronique. Selon l'invention, le procédé comprend deux étapes de calcul dissociées. Une étape A consiste
à - calculer des couples de nombres premiers (p, q), ce calcul est indépendant de la connaissance du couple (e, l) e l'exposant public
et l la longueur de la clé du procédé de cryptographie et à - stocker les couples ainsi obtenus. Une étape B très rapide qui peut être
exécutée en temps réel par le dispositif, consiste à calculer une clé d à partir des résultats de l'étape A et de la connaissance du couple
(e, l).

WO 2004/002058 A2